

CLAIMS:

What is claimed is:

1 1. A system for accessing and executing instruction sequences in a
2 physical memory from a virtual memory in a processor-based system, comprising:
3 a memory for storing instruction sequences by which the processor-
4 based system is processed, the memory including a physical memory and a virtual
5 memory; and
6 a processor for executing the stored instruction sequences; and
7 wherein the stored instruction sequences include process steps to cause
8 the processor to: (a) map a plurality of predetermined instruction sequences from
9 the physical memory to the virtual memory; (b) determine an offset to one of said
10 plurality of predetermined instruction sequences in the virtual memory; (c) receive
11 an instruction to execute the one of said plurality of predetermined instruction
12 sequences; (d) transfer control to the one of said plurality of predetermined
13 instruction sequences; and (e) process the one of said plurality of predetermined
14 instruction sequences from the virtual memory.

1 2. The system of Claim 1, wherein in step (c), the instruction is made
2 from an application program.

1 3. The system of Claim 1, wherein in step (c), the instruction is made
2 from a class driver.

1 4. The system of Claim 1, wherein step (a) comprises the steps of:
2 (a.1) mapping a plurality of BIOS instruction sequences from the
3 physical memory to the virtual memory, said BIOS instruction sequences including
4 a BIOS service directory; and
5 (a.2) mapping BIOS data from the physical memory to the virtual
6 memory.

1 5. The system of Claim 4, wherein step (b) comprises the steps of:
2 (b.1) determining a starting virtual address of the BIOS service
3 directory; and
4 (b.2) determining a starting virtual address of one of the plurality of
5 BIOS instruction sequences by reference to the BIOS service directory.

1 6. The system of Claim 5, wherein step (d) comprises the steps of:
2 (d.1) creating a register stack in a memory location;
3 (d.2) identifying a location of the starting virtual address of one of the
4 plurality of BIOS instruction sequences in the register stack; and
5 (d.3) transferring control to the one of the plurality of BIOS instruction
6 sequences.

1 7. The system of Claim 6, wherein in step (d.1), the memory location is a
2 buffer located in a dynamic random access memory (DRAM).

1 8. The system of Claim 6, wherein in step (d.1), the memory location is a
2 buffer located in a main memory.

1 9. The system of Claim 6, wherein step (e) comprises the steps of:
2 (e.1) determining if the starting virtual address is within a range of
3 addresses mapped from the physical memory to the virtual memory; and
4 (e.2) if so, executing the one of the plurality of BIOS instruction
5 sequences from the virtual memory, otherwise indicating that the starting virtual
6 address is not within the range of addresses mapped from the physical memory to
7 the virtual memory.

1 10. A method for accessing and executing instruction sequences in physical
2 memory from virtual memory in a processor-based system, comprising the steps of:

3 (a) mapping a plurality of predetermined instruction sequences from
4 the physical memory to the virtual memory;

5 (b) determining an offset to one of said plurality of predetermined
6 instruction sequences in the virtual memory;

7 (c) receiving an instruction to execute the one of said plurality of
8 predetermined instruction sequences;

9 (d) transferring control to the one of said plurality of predetermined
10 instruction sequences; and

11 (e) processing the one of said plurality of predetermined instruction
12 sequences from the virtual memory.

1 11. The method of Claim 10, wherein in step (c), the instruction is made
2 from an application program.

1 12. The method of Claim 10, wherein in step (c), the instruction is made
2 from a class driver.

1 13. The method of Claim 10, wherein step (a) comprises the steps of:

2 (a.1) mapping a plurality of BIOS instruction sequences from the
3 physical memory to the virtual memory, said BIOS instruction sequences including
4 a BIOS service directory; and

5 (a.2) mapping BIOS data from the physical memory to the virtual
6 memory.

7 14. The method of Claim 13, wherein step (b) comprises the steps of:

8 (b.1) determining a starting virtual address of the BIOS service
9 directory; and

10 (b.2) determining a starting virtual address of one of the plurality of
11 BIOS instruction sequences by reference to the BIOS service directory.

1 15. The method of Claim 14, wherein step (d) comprises the steps of:

2 (d.1) creating a register stack in a memory location;

3 (d.2) identifying a location of the starting virtual address of one of the
4 plurality of BIOS instruction sequences in the register stack; and

5 (d.3) transferring control to the one of the plurality of BIOS instruction
6 sequences.

1 16. The method of Claim 15, wherein in step (d.1), the memory location is
2 a buffer located in a dynamic random access memory (DRAM).

1 17. The method of Claim 15, wherein in step (d.1), the memory location is
2 a buffer located in a main memory.

1 18. The method of Claim 15, wherein step (e) comprises the steps of:
2 (e.1) determining if the starting virtual address is within a range of
3 addresses mapped from the physical memory to the virtual memory; and
4 (e.2) if so, executing the one of the plurality of BIOS instruction
5 sequences from the virtual memory, otherwise indicating that the starting virtual
6 address is not within the range of addresses mapped from the physical memory to
7 the virtual memory.

1 19. Computer-executable process steps for accessing and executing
2 instruction sequences in physical memory from virtual memory in a processor-
3 based system, the process steps including:

4 (a) mapping a plurality of predetermined instruction sequences
5 from the physical memory to the virtual memory;

6 (b) determining an offset to one of said plurality of predetermined
7 instruction sequences in the virtual memory;

8 (c) receiving an instruction to execute the one of said plurality of
9 predetermined instruction sequences;

10 (d) transferring control to the one of said plurality of predetermined
11 instruction sequences; and

12 (e) processing the one of said plurality of predetermined instruction
13 sequences from the virtual memory.

1 20. Computer-executable process steps of Claim 19, wherein in step (c), the
2 instruction is made from an application program.

1 21. Computer-executable process steps of Claim 19, wherein step (a)
2 comprises the steps of:

3 (a.1) mapping a plurality of BIOS instruction sequences from the
4 physical memory to the virtual memory, said BIOS instruction sequences including
5 a BIOS service directory; and

6 (a.2) mapping BIOS data from the physical memory to the virtual
7 memory.

1 22. Computer-executable process steps of Claim 21, wherein step (b)
2 comprises the steps of:

3 (b.1) determining a starting virtual address of the BIOS service
4 directory; and

5 (b.2) determining a starting virtual address of one of the plurality of
6 BIOS instruction sequences by reference to the BIOS service directory.

1 23. Computer-executable process steps of Claim 22, wherein step (d)
2 comprises the steps of:
3 (d.1) creating a register stack in a memory location;
4 (d.2) identifying a location of the starting virtual address of one of the
5 plurality of BIOS instruction sequences in the register stack; and
6 (d.3) transferring control to the one of the plurality of BIOS instruction
7 sequences.

1 24. Computer-executable process steps of Claim 23, wherein in step (d.1),
2 the memory location is a buffer located in a dynamic random access memory
3 (DRAM).

1 25. Computer-executable process steps in Claim 23, wherein in step (d.1),
2 the memory location is a buffer located in a main memory.

1 26. Computer-executable process steps of Claim 23, wherein step (e)
2 comprises the steps of:
3 (e.1) determining if the starting virtual address is within a range of
4 addresses mapped from the physical memory to the virtual memory; and
5 (e.2) if so, executing the one of the plurality of BIOS instruction
6 sequences from the virtual memory, otherwise that the starting virtual address is
7 not within the range of addresses mapped from the physical memory to the virtual
8 memory.

1 27. A system for accessing instruction sequences in a physical memory
2 from a virtual memory in a processor-based system, comprising:
3 a memory for storing instruction sequences by which the processor-
4 based system is processed, the memory including a physical memory and a virtual
5 memory; and
6 a processor for executing the stored instruction sequences; and
7 wherein the stored instruction sequences include process steps to cause
8 the processor to: (a) map a plurality of predetermined instruction sequences from
9 the physical memory to the virtual memory; (b) determine an offset to one of said
10 plurality of predetermined instruction sequences in the virtual memory; (c) receive
11 an instruction to execute the one of said plurality of predetermined instruction
12 sequences; (d) transfer control to the one of said plurality of predetermined
13 instruction sequences; and (e) process the one of said plurality of predetermined
14 instruction sequences from the virtual memory.

1 28. The system of Claim 27, wherein step (a) comprises the steps of:
2 (a.1) mapping a plurality of BIOS instruction sequences from the
3 physical memory to the virtual memory, said BIOS instruction sequences including
4 a plurality of BIOS read only memory (ROM) instruction sequences and a BIOS
5 service directory; and
6 (a.2) mapping BIOS data from the physical memory to the virtual
7 memory.

1 29. The system of Claim 28, wherein step (b) comprises the steps of:
2 (b.1) determining a starting virtual address of the BIOS service
3 directory; and
4 (b.2) determining a starting virtual address of one of the plurality of
5 BIOS instruction sequences by reference to the BIOS service directory.

1 30. The system of Claim 29, wherein step (d) comprises the steps of:
2 (d.1) creating a register stack in a memory location and;
3 (d.2) identifying a location of the starting virtual address of one of the
4 plurality of BIOS ROM instruction sequences in the register stack.

1 31. The system of Claim 30, wherein step (e) comprises the steps of:
2 (e.1) determining if the starting virtual address is within a range of
3 addresses mapped from the physical memory to the virtual memory; and
4 (e.2) if so, reading the one of the plurality of BIOS ROM instruction
5 sequences from the virtual memory, otherwise indicating that the starting virtual
6 address is not within the range of addresses mapped from the physical memory to
7 the virtual memory.

1 32. A method for accessing instruction sequences in physical memory
2 from virtual memory in a processor-based system, comprising the steps of:
3 (a) mapping a plurality of predetermined instruction sequences from
4 the physical memory to the virtual memory;

5 (b) determining an offset to one of said plurality of predetermined
6 instruction sequences in the virtual memory;
7 (c) receiving an instruction to execute the one of said plurality of
8 predetermined instruction sequences;
9 (d) transferring control to the one of said plurality of predetermined
10 instruction sequences; and
11 (e) processing the one of said plurality of predetermined instruction
12 sequences from the virtual memory.

1 33. The method of Claim 32, wherein step (a) comprises the steps of:
2 (a.1) mapping a plurality of BIOS instruction sequences from the
3 physical memory to the virtual memory, said BIOS instruction sequences including
4 a plurality of BIOS read only memory (ROM) instruction sequences and a BIOS
5 service directory; and
6 (a.2) mapping BIOS data from the physical memory to the virtual
7 memory.

1 34. The method of Claim 33, wherein step (b) comprises the steps of:
2 (b.1) determining a starting virtual address of the BIOS service
3 directory; and
4 (b.2) determining a starting virtual address of one of the plurality of
5 BIOS instruction sequences by reference to the BIOS service directory.

1 35. The method of Claim 34, wherein step (d) comprises the steps of:

- 2 (d.1) creating a register stack in a memory location; and
3 (d.2) identifying a location of the starting virtual address of one of the
4 plurality of BIOS ROM instruction sequences in the register stack.

1 36. The method of Claim 35, wherein step (e) comprises the steps of:

2 (e.1) determining if the starting virtual address is within a range of
3 addresses mapped from the physical memory to the virtual memory; and

4 (e.2) if so, reading the one of the plurality of BIOS ROM instruction
5 sequences from the virtual memory, otherwise indicating that the starting virtual
6 address is not within the range of addresses mapped from the physical memory to
7 the virtual memory.

1 37. A system to securely utilize Basic Input and Output System (BIOS)
2 services, comprising:

3 an access driver to generate a service request to utilize BIOS services,
4 the service request including a service request signature created using a private key
5 in a cryptographic key pair; and

6 an interface to verify the service request signature using a public key in
7 the cryptographic key pair to ensure the integrity of the service request.

1 38. The system of Claim 37, wherein:

2 the access driver generates a session request to establish a session with
3 the interface; and

4 the session request includes a session request signature created using a
5 private key in a cryptographic key pair.

1 39. The system of Claim 37, wherein:

2 the access driver generates a session request to end the session with the
3 interface; and

4 the session request includes a session request signature created using a
5 private key in a cryptographic key pair.

6 40. The system of Claim 37, wherein:

7 the interface generates an authority certificate and sends the authority
8 certificate to the access driver after receiving a session request; and

9 the access driver uses information included in the authority certificate to
10 generate subsequent session requests.

11 41. The system of Claim 40, wherein the authority certificate includes a
12 new public key.

1 42. The system of Claim 40, wherein the authority certificate includes a
2 new private key.

1 43. The system of Claim 40, wherein the authority certificate includes a
2 certificate signature.

1 44. The system of Claim 37, wherein:
2 the interface generates an authority certificate and sends the authority
3 certificate to the access driver after receiving the service request; and
4 the access driver uses information in the authority certificate to generate
5 subsequent service requests.

1 45. A method to securely invoke Basic Input and Output System (BIOS)
2 services, comprising:
3 creating a service request to invoke BIOS services;
4 signing the service request with a service request signature generated
5 using a private key in a cryptographic key pair; and
6 verifying the service request signature using a public key in the
7 cryptographic key pair to ensure the integrity of the service request.

1 46. The method of Claim 45, further comprising:
2 creating an authority certificate that includes a new private key and a
3 new public key after processing the service request;
4 signing a subsequent service request with a service request signature
5 generated using the new private key; and
6 verifying the service request signature of the subsequent service
7 request using the new public key.

1 47. The method of Claim 45, further comprising:

performing a BIOS service indicated by a service operation code
included in the service request.

48. The method of Claim 45, further comprising:

creating a session request to establish a session with a ROM Application
Program Interface (RAPI);

signing the session request with a session request signature generated
using a private key in a cryptographic key pair; and

verifying the session request signature using a public key in the
cryptographic key pair to ensure the integrity of the session request.

49. The method of Claim 48, further comprising:

creating an authority certificate that includes a new private key and a
new public key after processing the session request;

signing a subsequent session request with a session request signature
generated using the new private key; and

verifying the session request signature of the subsequent session
request using the new public key.

50. The method of Claim 45, further comprising:

creating a session request to end a session with a ROM Application
Program Interface (RAPI);

signing the session request with a session request signature generated
using a private key in a cryptographic key pair; and

6 verifying the session request signature using a public key in the
7 cryptographic key pair to ensure the integrity of the session request.

1 51. A computer program embodied on a computer-readable medium to
2 securely utilize Basic Input and Output System (BIOS) services, comprising:
3 an access driver to generate a service request to utilize BIOS services,
4 the service request including a service request signature created using a private key
5 in a cryptographic key pair; and
6 an interface to verify the service request signature using a public key in
7 the cryptographic key pair to ensure the integrity of the service request.

1 52. A computer data signal embodied in a data stream, comprising:
2 an access driver to generate a service request to utilize BIOS services,
3 the service request including a service request signature created using a private key
4 in a cryptographic key pair; and
5 an interface to verify the service request signature using a public key in
6 the cryptographic key pair to ensure the integrity of the service request.